

# 14-2985-cv

---

IN THE  
**United States Court of Appeals**  
FOR THE SECOND CIRCUIT

---

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT  
CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION,

---

MICROSOFT CORPORATION,

*Appellant,*

—v.—

UNITED STATES OF AMERICA

*Appellee.*

---

ON APPEAL FROM THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK

---

**BRIEF OF *AMICUS CURIAE* JAN PHILIPP ALBRECHT, MEMBER OF THE  
EUROPEAN PARLIAMENT**

---

Owen C. Pell  
Ian S. Forrester, Q.C.  
Paige C. Spencer  
WHITE & CASE  
1155 Avenue of the Americas  
New York, New York 10036  
212-819-8891

*Counsel for Amicus Curiae Jan Philipp  
Albrecht*

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
STATEMENT OF INTEREST OF THE AMICUS CURIAE .....	3
SUMMARY OF ARGUMENT .....	4
ARGUMENT .....	5
CONCLUSION .....	12

## TABLE OF AUTHORITIES

	<u>Page</u>
<b>TREATIES AND STATUTES</b>	
Charter on Fundamental Rights of the European Union, art. 8, Mar. 30, 2010, 2010 O.J. (C83) 389.....	6, 7
Consolidated Version of the Treaty on European Union, art. 6, May 9, 2008, 2008 O.J. (C115) 15.....	7
Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol Numbers 11 and 14, Jun. 1, 2010, C.E.T.S. No. 005. ....	7
Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. No. 108 .....	7
Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC) .....	6, 7, 9
Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC) .....	6
Treaty on the Functioning of the European Union, art. 294, Oct 26. 2012, 2012 O.J. (C326) 47.....	5, 6, 7
U.S.-European Union Agreement on Mutual Legal Assistance, <u>done</u> Jun. 23, 2003, T.I.A.S. No. 10-201.1 (2003).....	5, 6, 8 9, 10, 11, 12
<b>MISCELLANEOUS</b>	
EUROPEAN PARLIAMENT WEBSITE, <a href="http://www.europarl.europa.eu/">http://www.europarl.europa.eu/</a> (last visited Dec. 18, 2014) .....	5
Communication from the Commission to the European Parliament and to the Council, Rebuilding Trust in EU-US Data Flows, at 8, COM (2013) 846 final (Nov. 27, 2013).....	11
Report of the European Parliament Committee on Industry, Research and Energy on Unleashing the Potential of Cloud Computing, at 13-14 (Nov. 4, 2013), <u>available at</u> <a href="http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//EN">http://www.europarl.europa.eu/sides/getDoc.do?pubRef=- //EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//EN</a> .....	10, 11

**STATEMENT OF INTEREST OF THE AMICUS CURIAE**<sup>1</sup>

Jan Philipp Albrecht is a Member of the European Parliament (“MEP”) from Germany. He has been a Member of the European Parliament since 2009. He holds degrees in information and communications technology law from the Universities of Hanover and Oslo.

MEP Albrecht serves as vice-chair of the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs, which is responsible for civil rights legislation, including with regard to personal data processing. He also serves on the Committee on the Internal Market and Consumer Protection, which is responsible for, inter alia, consumer protection in the field of electronic commerce.

MEP Albrecht serves as standing rapporteur of the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs for the Transatlantic Trade and Investment Partnership (“TTIP”) and is therefore responsible, inter alia, for the personal data protection aspects of this agreement currently under negotiation.

MEP Albrecht has also actively participated in the European Parliament’s considerations of data-sharing agreements with the United States of America (“U.S.”) under which the European Union (“EU”) provides for the transfer of European bank

---

<sup>1</sup> This brief is filed with the written consent of all parties. No counsel for a party authored this brief in whole or in part, nor did any person or entity, other than *Amicus* or its counsel, make a monetary contribution to the preparation or submission of this brief.

data for use in the U.S. Terrorist Finance Tracking Program and for the transfer of Passenger Name Records to the United States Department of Homeland Security.

MEP Albrecht maintains a particular expertise and interest in the fields of civil rights and data protection. He serves as rapporteur of the European Parliament for the European Commission's proposed General Data Protection Regulation, which would unify data protection requirements within the EU, including the requirements for transferring personal data to third countries such as the United States. He also serves as the rapporteur of the European Parliament for the agreement between the EU and the United States on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters ("umbrella" agreement), which is currently under negotiation. Given his knowledge on this issue, MEP Albrecht has been joined in this submission by Marju Lauristin, another MEP with specific knowledge in this area, underscoring the importance of the issues presented by this case under European law.

### **SUMMARY OF ARGUMENT**

Personal data located in EU territory is subject to strict rules designed to maintain the autonomy of the affected individual (data subject). Those rules apply to the email account covered by the warrant in issue in this case. They balance the

protection of the individual's rights with the necessity of data processing for public interests, such as law enforcement.

The rules governing the handling of personal data in the EU reflect the high level of sensitivity on the part of EU citizens and regulators about the protection of personal data. That sensitivity, and the differences between EU and U.S. rules on data protection, have been expressly acknowledged by the executive branches of government in the U.S. and in the EU in the conclusion of the U.S.-EU Agreement on Mutual Legal Assistance, done June 23, 2003, T.I.A.S. No. 10-201.1 (2003) ("EU MLAT"). The mechanisms established by the EU MLAT are expressly designed to permit U.S. law enforcement authorities to obtain personal data located in the EU for use in criminal investigation. By upholding the warrant at issue, the District Court endorsed the by-passing of the EU MLAT and the respect for foreign jurisdiction inherent therein.

### **ARGUMENT**

The European Parliament is the Parliament of the EU. It consists of 751 directly elected Members ("MEPs") who represent the 500 million European Citizens in the 28 different EU Member States.<sup>2</sup> Under Article 294 of the Treaty

---

<sup>2</sup> EUROPEAN PARLIAMENT WEBSITE, <http://www.europarl.europa.eu/> (last visited Dec. 18, 2014).

on the Functioning of the European Union (“TFEU”)<sup>3</sup> the European Parliament has co-decision power in all areas of legislation (together with the Council of the European Union, which consists of the ministers of the governments of the Member States). The European Parliament also has significant powers in respect of the conclusion of international agreements (like the EU MLAT) and the appointment of the executive branch of the European Union (the European Commission).

The European Parliament has long advocated the protection of privacy and personal data. The first EU directive on data protection<sup>4</sup> (“Data Protection Directive”) was passed in 1995 to reconcile and harmonize the different approaches to data protection that had evolved in the EU Member States. Its provisions were supplemented in 2002 by the ePrivacy Directive.<sup>5</sup> This framework is currently under review and will be replaced by a single, new legislative act. As noted, MEP Albrecht is the parliamentary rapporteur, charged with following the new measure through its legislative stages.

Whilst the Directives lay down a framework for the specifics of data protection law across the EU, the basic principle of confidentiality of personal data is enshrined as a human right in the European Union Charter on Fundamental

---

<sup>3</sup> Treaty on the Functioning of the European Union, art. 294, Oct 26. 2012, 2012 O.J. (C326) 47.

<sup>4</sup> Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

<sup>5</sup> Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

Rights (“Charter”).<sup>6</sup> Under Article 6(1) of the Treaty on European Union (“TEU”),<sup>7</sup> the Charter has a status equal to the Treaties of the European Union, whilst the provisions of the European Convention on Human Rights<sup>8</sup> constitute general principles of EU Law.<sup>9</sup> In addition, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data<sup>10</sup> also underlines that data protection, as a fundamental right, is a common principle in Europe.

These rules seek to achieve a balance between the preservation of self-determination, personal dignity, and the integrity of the individual, and the facilitation of the free flow of data. The European rules also contain exceptions to ensure that the rights of the individual do not unjustifiably obstruct the legitimate activities of Member States in the fields of security and law enforcement.<sup>11</sup>

The protection of privacy and personal data in EU law is not intended to stop the use and exchange of data. Its purpose is to regulate the transfer and storage of data, preserving the ability of the data subject to control his personal data. Interference with that control is limited to circumstances where it is necessary,

---

<sup>6</sup> Charter on Fundamental Rights of the European Union, art. 8, Mar. 30, 2010, 2010 O.J. (C83) 389.

<sup>7</sup> Consolidated Version of the Treaty on European Union, art. 6(1), May 9, 2008, 2008 O.J. (C 115) 15.

<sup>8</sup> Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol Numbers 11 and 14, June 1, 2010, C.E.T.S. No. 005.

<sup>9</sup> TEU art. 6(3).

<sup>10</sup> Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, C.E.T.S. No. 108.

<sup>11</sup> Data Protection Directive, supra note 4, at 39.



proportionate, and subject to effective oversight—precisely as contemplated by the EU MLAT. The decision of the District Court effectively permits this carefully constructed regime to be sidestepped. It has far reaching implications for the handling of personal data by the globalized technology industry.

European citizens are highly sensitive to the differences between European and U.S. standards on data protection. Such concerns are frequently raised in relation to the regulation of cross-border data flows and the mass-processing of data by U.S. technology companies. The successful execution of the warrant at issue in this case would extend the scope of this anxiety to a sizeable majority of the data held in the world's datacenters outside the U.S. (most of which are controlled by U.S. corporations) and would thus undermine the protections of the EU data protection regime, even for data belonging to an EU citizen and stored in an EU country.

This case concerns an email account located in a datacenter in Ireland.<sup>12</sup> The content of that email account is located inside the EU and the customer therefore must benefit from the protections of EU law. Since Ireland hosts many datacenters operated by corporate groups whose headquarters are located in the United States, the present case is relevant for a gigantic volume of data held on behalf millions of EU citizens. One of the protections is that the data will not be transferred to a

---

<sup>12</sup> See Appendix (“A”) at (A37, A40).

country outside the EU unless the recipient has in place safeguards to ensure that the data will receive equivalent protection to that which it is afforded in the EU.<sup>13</sup> Under these provisions the transfer by Microsoft of the content of the email account from Ireland to the United States is not permitted by EU law. However, the criminal law exceptions in the European directives, including as covered by the EU MLAT procedures, would permit Irish law enforcement authorities to obtain the information, but do not permit Microsoft to send the data to the U.S. to be handed to the U.S. Attorney there.

Even if, contrary to the Appellant's case, the warrant at issue is capable of applying to the content of the email account, this would nevertheless give rise to a conflict of jurisdiction. Microsoft would be required by the warrant, yet it is not permitted under EU law to transfer the contents of the email account to the U.S. It is the recognition of such conflicts that led to the conclusion of the EU MLAT.<sup>14</sup> The EU MLAT provides a straightforward mechanism for cooperation between the U.S. authorities and the authorities of the Member State in which the information sought is located (in this case Ireland). That mechanism permits the Member State's authorities to exercise powers, in full compliance with EU data protection

---

<sup>13</sup> Data Protection Directive, supra note 4, at 45.

<sup>14</sup> U.S.-European Union Agreement on Mutual Legal Assistance, done Jun. 23, 2003, T.I.A.S. No. 10-201.1 (2003).

rules, to search for and seize personal data for the purpose of a criminal investigation, and to pass that information to the U.S. Attorney.<sup>15</sup>

By ignoring this mechanism, the District Court dismisses the relevance and applicability of an instrument expressly designed to overcome the precise issues which arise in this case, i.e., a conflict arising out of the recognized differences in the data protection regimes in the U.S. and EU.<sup>16</sup>

It is fair to record that there are major differences between the U.S. and European laws on data protection. The European standard is much more severe than the U.S. standard. Both policies are a legitimate manifestation of legislative and regulatory choices, so it is not necessary to conclude that one is too strict or not strict enough. The principal conclusion to draw is that they are *very different*. European law in effect forbids the transfer of personal data to third countries (including the United States) unless the recipient has established ‘European-style’ protections to ensure its privacy. For U.S. law to treat data stored in Europe as if it were stored in the United States is a territorial encroachment without justification, and one which is exacerbated by the sharp differences in the legal status of personal data in the U.S. and the EU.

The European Parliament has already noted the practice whereby, for example, a U.S. prosecutor ignores the EU MLAT and seeks to compel the

---

<sup>15</sup> MLAT, art. 8.

<sup>16</sup> *Id.*, Explanatory Note.

disclosure of personal data belonging to an EU citizen by a technology company.<sup>17</sup> This unilateral exercise of jurisdiction over data held in the EU puts into serious jeopardy the level of trust between the EU and U.S. on data protection matters.<sup>18</sup> Such trust is essential for the conclusion of future agreements between the EU and U.S. on cooperation in law enforcement. Moreover, the European Commission has indicated that it would seek, in negotiations on a U.S.-EU “umbrella” agreement on transfers and processing of personal information in the context of police and judicial cooperation in criminal matters, further clarification that U.S. authorities will not seek to directly access data stored in the EU outside formal channels such as the EU MLAT.<sup>19</sup> The upholding of the warrant in this case would forestall this future agreement and disturb these negotiations.

The refusal of the U.S. Attorney to recognize that the email account at issue is located in a foreign jurisdiction and subject to foreign data protection rules is not only offensive to the sensitivities of European citizens but also reinforces the already strong sentiment of many EU citizens that their data is not “safe” when they use IT services offered by U.S. corporations. Sentiment such as this creates

---

<sup>17</sup> Report of the European Parliament Committee on Industry, Research and Energy on unleashing the potential of cloud computing, at 13-14 (Nov. 4, 2013), available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0353+0+DOC+PDF+V0//EN>.

<sup>18</sup> *Id.*

<sup>19</sup> See generally, Communication from the Commission to the European Parliament and to the Council, Rebuilding Trust in EU-US Data Flows, COM (2013) 846 final (Nov. 27, 2013).

major obstacles to the negotiation of agreements between the EU and U.S. relating to closer cooperation in both law enforcement, and in trade. The regulation of data flows is an important issue in the negotiations regarding TTIP and the Trade in Services Agreement. The District Court's failure to recognize the significance of the location of the email account at issue, and accordingly the EU rules to which it is subject, is an unfortunate occurrence which has the potential to damage political and trade relations. This is particularly the case where the executive branches of both the U.S. and the EU have acknowledged that the differing data protection regimes in these two jurisdictions are a relevant consideration in law enforcement and concluded the EU MLAT with the express intention of creating a mechanism to respect these differences, without obstructing law enforcement activity.

### **CONCLUSION**

For the foregoing reasons, *Amicus Curiae* MEP Jan Philipp Albrecht urges the Court to reverse the District Court's decision, and order the United States to proceed under the U.S.-Ireland Mutual Legal Assistance Treaty.

Dated: December 19, 2014

By: /s/ Owen C. Pell  
Owen C. Pell  
Ian S. Forrester, Q.C.  
Paige C. Spencer  
WHITE & CASE  
1155 Avenue of the Americas  
New York, New York 10036  
212-819-8891

*Counsel for Amicus Curiae*  
*Jan Philipp Albrecht*

**Certification of Compliance with Type-Volume Limitation, Typeface Requirements and Type Style Requirements**

1. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(7)(B) because it contains **2,379** words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionately-spaced typeface using Microsoft Word, 14 point font size.

Dated: December 19, 2014

WHITE & CASE LLP

By: /s/ Owen C. Pell

Owen C. Pell

Ian S. Forrester, Q.C.

Paige C. Spencer

1155 Avenue of the Americas

New York, New York 10036

Telephone: (212) 819-8891

Facsimile: (212) 354-8113

*Counsel for Jan Philipp Albrecht*

### **Certificate of Service**

I hereby certify that on this 19<sup>th</sup> day of December 2014, a true and correct copy of the foregoing Brief was served on all counsel of record via ECF pursuant to Local Rule 25.1(h).

Dated: December 19, 2014

WHITE & CASE LLP

By: /s/ Owen C. Pell

Owen C. Pell

Ian S. Forrester, Q.C.

Paige C. Spencer

1155 Avenue of the Americas

New York, New York 10036

Telephone: (212) 819-8200

Facsimile: (212) 354-8113

*Counsel for Jan Philipp Albrecht*